



World Wide Technology, Inc.

Migrating from the Cisco Pix Firewall to the Cisco ASA Security Appliance

The
Vision
to Succeed



Presented by:

David Harrison - CCIE #8521, CCSP, CCSI
Ladi Adefala, CCSI
Ashish Upadhyay, BDM

Date:
March 13, 2008



- ☐ Introductions
- ☐ Cisco PIX - End of Sale Overview
- ☐ Cisco ASA Product Overview
- ☐ Key PIX to ASA Migration Drivers
- ☐ Cisco PIX-2-ASA Feature Comparison Overview
- ☐ How to Migrate from PIX to ASA Platform? Step-by-Step Approach
- ☐ WWT Security Professional Services Overview
- ☐ Important Links/Reference Documents
- ☐ Q&A

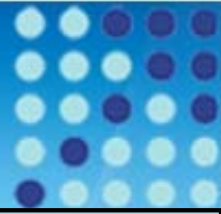




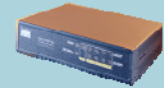
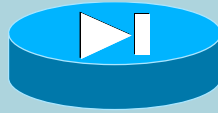
- WWT Security Practice Team:
 - Ashish Upadhyay, Business Development Manager
 - Dave Harrison, CCIE #8521, CCSP, CCSI – National Security Lead
 - Ladi Adefala, CCSI – National Post-Sales Practice Manager
 - Sara Vaughan – Marketing/Event Coordination
 - Ed Levens/Diana Dewerey – Marketing/Event Support
- Cisco Guests
 - Scott Maxwell, AT-CAM Commercial/Enterprise
 - Brian Sak, Virtual Security Expert
 - Tim St. Laurent, AT-CAM Federal
 - Daniel Charborneau, Channel SE



Which Products are Going End of Sale?



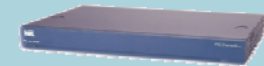
- All models of the Cisco PIX Security Appliance product family
 - Cisco PIX 501
 - Cisco PIX 506E
 - Cisco PIX 515E
 - Cisco PIX 525
 - Cisco PIX 535
- All Cisco PIX Security Appliance Software release trains
 - 6.2, 6.3, 7.0, 7.1, 7.2, and 8.0
- The following accessories will be sold for six months past chassis/bundle end of sales
 - Licenses
 - I/O cards and VAC+ card
 - Memory upgrade kits
 - Accessory kitsf



Cisco PIX 501



Cisco PIX 506E



Cisco PIX 515E



Cisco PIX 525



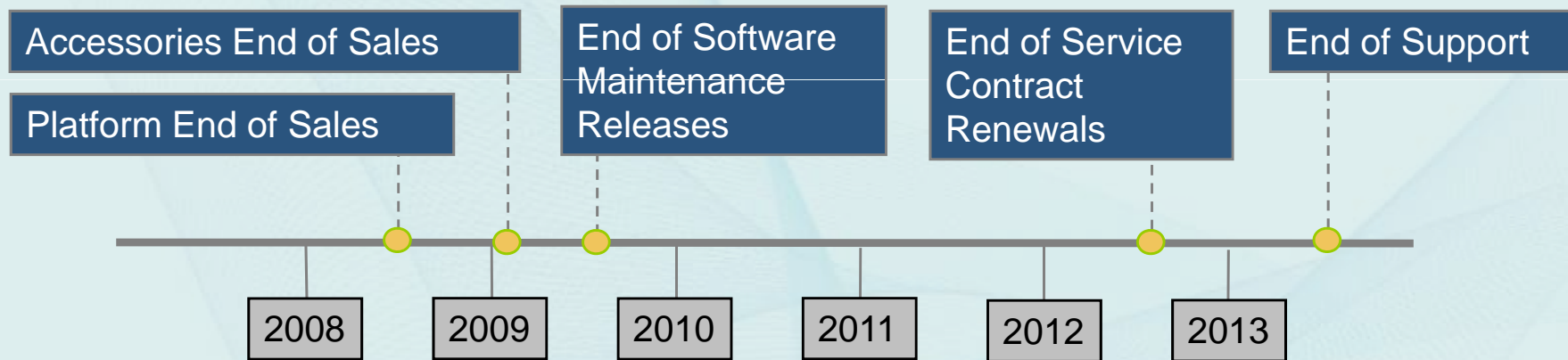
Cisco PIX 535



Cisco PIX Security Appliance Product Family

End of Sale Timeline

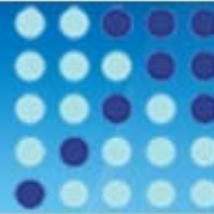
The
Vision
to Succeed



Milestone	Date
External announcement	January 28, 2008
End of Sales (EoS) for platforms/bundles	July 28, 2008
End of Sales (EoS) for accessories	January 27, 2009
End of software maintenance releases	July 28, 2009
End of service contract renewals	October 23, 2012
End of Support / End of Life (EoL)	July 27, 2013



Which Products are Going End of Sale?



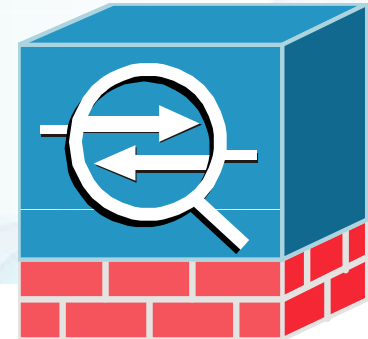
End-of-Life Milestones and Dates for the Cisco VPN 3000 Series Concentrators

Milestone	Definition	Date
End-of-Life Announcement Date	The date the document that announces the end of sale and end of life of a product is distributed to the general public.	February 7, 2007
End-of-Sale Date	The last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale after this date.	August 6, 2007
Last Ship Date: HW	The last-possible ship date that can be requested of Cisco and/or its contract manufacturers. Actual ship date is dependent on lead time.	November 4, 2007
End of Routine Failure Analysis Date: HW	The last-possible date a routine failure analysis may be performed to determine the cause of product failure or defect.	August 5, 2008
End of New Service Attachment Date: HW	For equipment and software that is not covered by a service-and-support contract, this is the last date to order a new service-and-support contract or add the equipment and/or software to an existing service-and-support contract.	August 5, 2008
End of Service Contract Renewal Date: HW	The last date to extend or renew a service contract for the product.	November 1, 2011
Last Date of Support: HW	The last date to receive service and support for the product. After this date, all support services for the product are unavailable, and the product becomes obsolete.	August 4, 2012





1. Advanced Firewall Services
2. Unified Communications Security
3. SSL and IPSEC VPN
4. Intrusion Prevention
5. Content Security Services
 - Anti Virus
 - Anti Spam
 - Anti Phishing
 - Anti Spyware
 - URL filtering



Why announce the end of sale now?



- Increased frequency and sophistication of Network attacks – Enterprise Security needs be evolved.
- Regulatory Compliance Pressure – Network Security as part of day-to-day operations of a business
- New network demands caused by - New applications such as unified communications, video, and collaboration require the next generation of networks and security.



Your Network and Threats to Your Network Have Changed...

The
Vision
to Succeed



Increased and More Complex Threats

Convergence of
Data and Voice

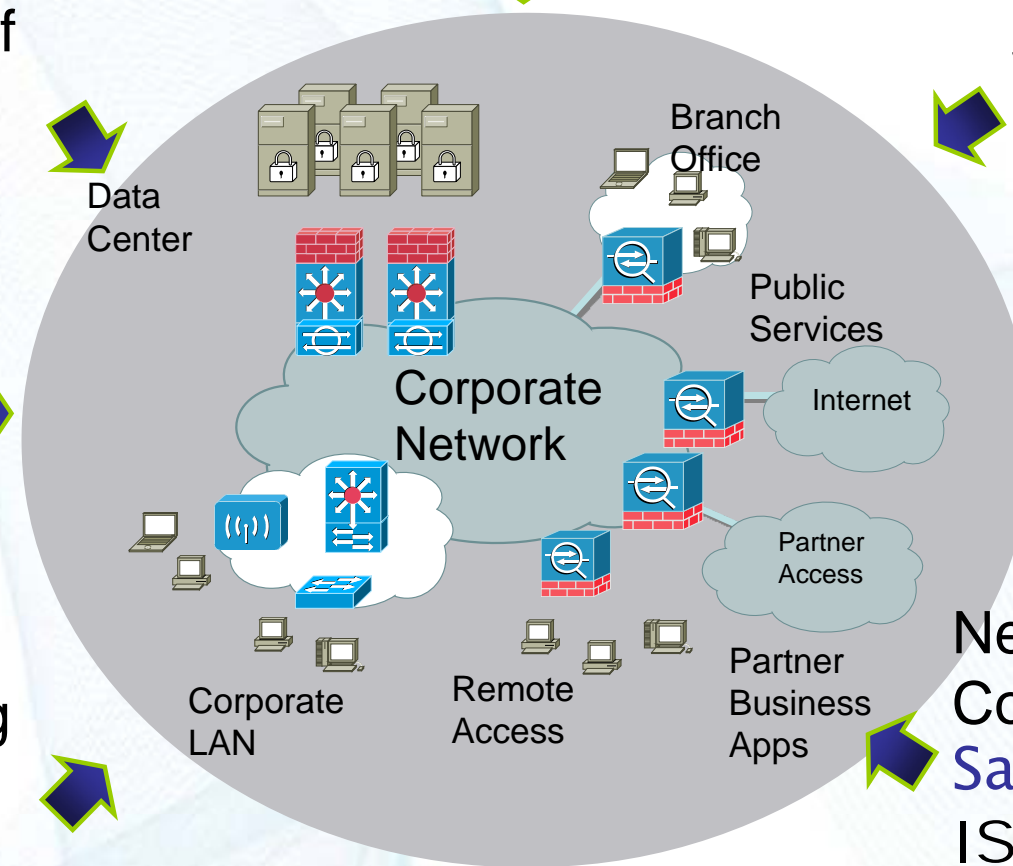
Wireless Mobility

More Media-Rich
Applications

New Focus on
Compliance
Sarbanes Oxley
ISO 27001
CobiT

Increase in
Online
Collaboration

Disappearing
Network
Perimeters



....Your Security Must Adapt as Well



Cisco ASA 5500 Series Appliances

Solutions Ranging from Desktop to Data Center



Cisco ASA 5500 Platforms

- Integrates, market-proven firewall, SSL/IPsec, IPS, and content security technologies
- Extensible multi-processor architecture delivers high concurrent services performance and significant investment protection
- Flexible management lowers cost of ownership
- Easy-to-use Web-based user interface
- Numerous certifications and awards
- And much more...



ASA 5505



ASA 5510



ASA 5520



ASA 5540



ASA 5550



ASA 5580-20



ASA 5580-40



New



New



Teleworker

Branch Office

Internet Edge

Campus Segmentation

Data Center



Recommended Migration Path for Cisco PIX Security Appliance Customers

The Vision 08
to Succeed

Cisco ASA 5505 Series



Cisco ASA 5510 / 5520 Series



Cisco ASA 5520 / 5540 Series



Cisco ASA 5550 / 5580 Series



Key Migration Benefits

- 1.5 - 2.5X firewall throughput
- 3 - 33X VPN throughput
- 8 port switch with 2 PoE ports
- VLAN support (20 with Sec+)
- Supports SSL VPN
- Modular for future upgrades

Key Migration Benefits

- 1.6 - 2.4x firewall throughput
- 2.3 - 3x scalability (conns/sec)
- Gigabit Ethernet support
- A/A solution costs 30% less
- VPN clustering/load balancing
- Supports IPS, CSC, SSL VPN

Key Migration Benefits

- 1.5 - 2x firewall throughput
- 1.3 - 2.7x scalability
- Supports 3X GigE density
- A/A solution costs 30% less
- VPN clustering/load balancing
- Supports IPS, CSC, SSL VPN

Key Migration Benefits

- 2 - 20x real-world FW throughput
- 2 - 8x scalability (conns/sec)
- Supports SSL VPN, inc. clus/LB
- 10GE I/O support (5580)
- Supports 2.5x GE density (5580)
- A/A solution costs 35% less

Cisco PIX 501 Series



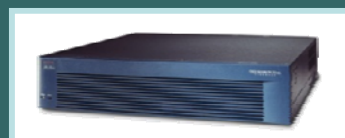
Cisco PIX 506E Series



Cisco PIX 515E Series










Cisco PIX 525 Series

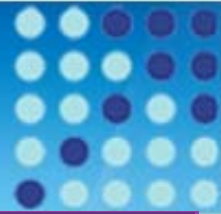


Cisco PIX 535 Series



Cisco ASA 5500 Series Model/License	5505 Base / Security Plus	5510 Base / Security Plus	5520	5540	5550	5580-20	5580-40
Product image (click to enlarge)							
Network location	Small Business, Branch Office, Enterprise Teleworker	Internet Edge	Internet Edge	Internet Edge	Internet Edge, Campus	Data Center, Campus	Data Center, Campus
Performance Summary							
Maximum firewall throughput	150 Mbps	300 Mbps	450 Mbps	650 Mbps	1.2 Gbps	5 Gbps (real-world HTTP), 10 Gbps (jumbo frames)	10 Gbps (real-world HTTP), 20 Gbps (jumbo frames)
Maximum firewall connections	10000 / 25,000	50,000 / 130,000	280,000	400,000	650,000	1,000,000	2,000,000
Maximum firewall connections/second	4000	9000	12,000	25,000	36,000	90,000	150,000
Packets per second (64 byte)	85,000	190,000	320,000	500,000	600,000	2,500,000	4,000,000
Maximum 3DES/AES VPN throughput	100 Mbps	170 Mbps	225 Mbps	325 Mbps	425 Mbps	1 Gbps	1 Gbps
Maximum site-to-site and remote access VPN sessions	10 / 25	250	750	5000	5000	10,000	10,000
Maximum SSL VPN user sessions¹	25	250	750	2500	5000	10,000	10,000
Bundled SSL VPN user session¹	2	2	2	2	2	2	2

Technical Summary	5505	5510	5520	5540	5550	5580-20	5580-40
Memory	256 MB	256 MB	512 MB	1 GB	4 GB	8 GB	12 GB
Minimum system flash	64 MB	64 MB	64 MB	64 MB	64 MB	1 GB	1 GB
Integrated ports²	8 port 10/100 switch with 2 Power over Ethernet ports	5-10/100 / 2-10/100/1000, 3-10/100 +4-10/100/1000, 4 SFP (with 4GE SSM)	4-10/100/1000, 1-10/100 +4-10/100/1000, 4 SFP (with 4GE SSM)	4-10/100/1000, 1-10/100 +4-10/100/1000, 4 SFP (with 4GE SSM)	8-10/100/1000, 4-SFP, 1-10/100	2-10/100/1000 Management +4-10/100/1000 (with ASA5580-4GE-CU) + 4 GE SR LC (with ASA5580-4GE-FI) +2 10GE SR LC (with ASA5580-2X10GE-SR)	2-10/100/1000 Management +4-10/100/1000 (with ASA5580-4GE-CU) + 4 GE SR LC (with ASA5580-4GE-FI) +2 10GE SR LC (with ASA5580-2X10GE-SR)
Maximum virtual interfaces (VLANs)	3 (trunking disabled) / 20 (trunking enabled)	50 / 100	150	200	250	100 (250 ⁵)	100 (250 ⁵)
Expansion Capabilities							
SSC/SSM/IC Expansion	1-SSC	1-SSM	1-SSM	1-SSM	Not Available	6-IC	6-IC
SSC/SSM/ICs supported	Future, SSC	CSC SSM, AIP SSM, 4GE SSM	CSC SSM, AIP SSM, 4GE SSM	CSC SSM, AIP SSM, 4GE SSM	Not Available	4-10/100/1000, 4-GE SR LC, 2-10GE SR LC	4-10/100/1000, 4-GE SR LC, 2-10GE SR LC
Intrusion Prevention	Not available	Yes (with AIP SSM)	Yes (with AIP SSM)	Yes (with AIP SSM)	Not Available	Not Available	Not Available



Many Compelling Benefits for Migrating to Cisco ASA 5500 Adaptive Security Appliances

Adaptive Security Offers Better, Flexible Protection



- Superior network protection from ever-changing threats through IPS, CSC, etc
- Equal or better pricing provides lower TCO
- Better performance and scalability, solutions scaling to 10+ Gbps
- Flexible VPN solution with market-leading SSL

Mature, Next-Generation Security Solution



- Built upon 10+ years of innovation in Cisco PIX, VPN 3000, and IPS 4200 solutions
- Hundreds of thousands of Cisco ASA 5500 units deployed worldwide
- GD quality software available (v7.0.7+)
- Common Criteria, FIPS, and NEBS certified

Leverages Customer's Existing PIX Investment



- Cisco PIX knowledge directly transferable to Cisco ASA 5500 Series
- Consistent GUI and CLI interfaces as Cisco PIX Security Appliances
- Consistent syslog and SNMP monitoring
- Managed by Cisco Security Manager, MARS, and many 3rd



Cisco ASA 5500 Series: Breadth and Depth

Industry First Scalable, Multi-Function, Feature Rich Appliance

The
Vision
to Succeed



Firewall with Application Layer Security



- Multi-layer packet and traffic analysis
- Advanced application and protocol inspection services
- Network application controls
- Advanced VoIP/multimedia security

IPS and Anti-X Defenses



- Real-time protection from application and OS level attacks
- Network-based worm and virus mitigation
- Spyware, adware, malware detection and control
- On-box event correlation and proactive response

Access Control and Authentication



- Flexible user and network based access control services
- Stateful packet inspection
- Integration with popular authentication sources including Microsoft Active Directory, LDAP, Kerberos, and RSA SecurID

SSL and IPSec Connectivity



- Threat protected SSL and IPSec VPN services
- Zero-touch, automatically updateable IPSec remote access
- Flexible clientless and full tunneling client SSL VPN services
- QoS/routing-enabled site-to-site VPN

Cisco Intelligent Networking Services



- Active\Active Failover
- Bridged Firewall
- Multicast support
- Virtual Firewalls\Multiple Context
- Network segmentation & partitioning
- Routing, resiliency, load-balancing



Cisco ASA 5500 Adaptive Security Appliances

Delivering Market-Leading Threat Defense and VPN Services

The
Vision
to Succeed



Provides Converged Threat Defense, Flexible Secure Connectivity,
Minimized Operation Costs, and Unique Adaptive Design to Combat Future Threats

Market-Leading Firewall Services

- Integrates and extends the #1 deployed firewall technology from Cisco PIX Security Appliances
- Built upon the experience of over one million PIX deployed worldwide and 10+ years of innovation

Market-Leading VPN Services

- Integrates and extends the #1 deployed remote access VPN technology from Cisco VPN 3000 Concentrators and Cisco PIX Security Appliances, offering both SSL and IPsec VPN services

Market-Leading IPS Services

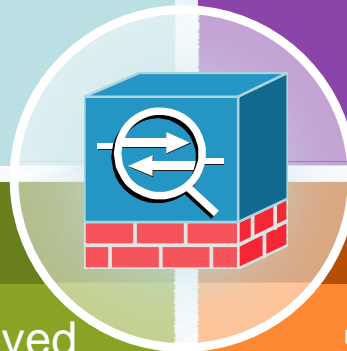
- Integrates and extends the #1 deployed IPS and IDS technology from the Cisco IPS 4200 Series
- Provides comprehensive security from directed attacks and many other threats

Market-Leading Content Security

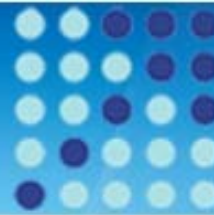
- Integrates and extends the #1 deployed gateway content security technology to protect from viruses, spyware, spam, phishing, and employee productivity impacting websites

Market-Leading Unified Communications Security

- Comprehensive access control, threat protection, network policies, service protection, and voice/video confidentiality for real-time Unified Communications traffic



Cisco ASA 5500 Series and Cisco PIX Security Appliances Feature Comparison



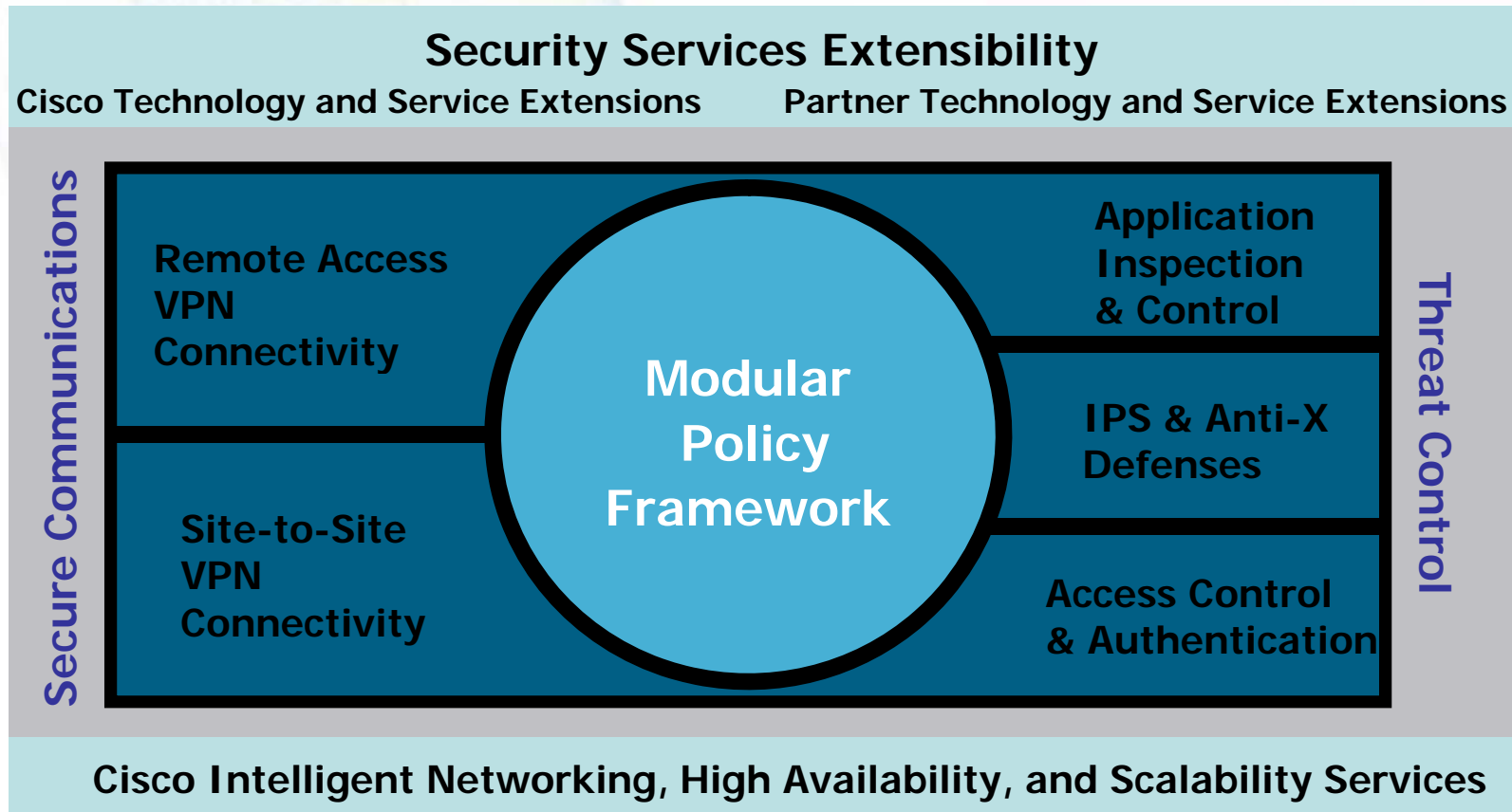
	Cisco PIX	Cisco ASA	Cisco ASA 5500 Benefit
Flexible Access Control , Both IP and User-Based	✓	✓	Cisco ASA 5500 Supports More ACLs due to Increased Memory
Advanced Application Layer Firewall Services for over 30 Popular Protocols	✓	✓	Cisco ASA 5500 Offers Better Deep Packet Inspection Performance
Security Services for Encrypted Voice / Video Communications	✗	✓	Only Cisco ASA 5500 Enables Secure End-to-End Encrypted Voice / Video Communications
Cisco Easy VPN and Site-to-Site IPsec VPN	✓	✓	Cisco ASA 5500 Provides Superior VPN Performance
Clientless SSL VPN and Cisco AnyConnect SSL VPN	✗	✓	Cisco ASA 5500 Provides World-Class, Flexible SSL VPN Access
VPN Clustering and Load Balancing Support	✗	✓	Cisco ASA 5500 Provides Enterprise-Class VPN Scalability
Full-Featured, Hardware Accelerated IPS Services	✗	✓	Cisco ASA 5500 Provides Superior Protection from Attacks
Anti-Virus, Anti-Spam, Anti-Phishing, and URL Filtering Services from Trend Micro	✗	✓	Cisco ASA 5500 Protects from Malware, Helping Increase Employee Productivity
Consistent Management and Monitoring	✓	✓	Leverage Cisco PIX Knowledge and Tools with Cisco ASA 5500



Cisco ASA 5500 Series Modular Policy Framework

Extensible Design Enables Flexible, Flow-Based Services Policies

The
Vision
to Succeed



The Cisco ASA 5500 Series Modular Policy Framework Allows Business to Adapt and Extend the Security Services Profile Via Cisco-Developed and Partner-Provided Innovations Delivering High Current Services Performance and Services Extensibility





Modular Policy Framework Overview

Modular Policy Framework provides a consistent and flexible way to configure security appliance features in a manner similar to Cisco IOS software QoS CLI. For example, you can use Modular Policy Framework to create a timeout configuration that is specific to a particular TCP application, as opposed to one that applies to all TCP applications.

Modular Policy Framework is supported with these features:

- IPS
- TCP normalization, and connection limits and timeouts
- QoS policing
- QoS priority queue
- Application inspection

Configuring Modular Policy Framework consists of three tasks:

1. Identify the traffic to which you want to apply actions. See "**Using a Class Map**"
2. Apply actions to the traffic. See "[Defining Actions Using a Policy Map](#)" section.
3. Activate the actions on an interface. See "[Applying a Policy to an Interface Using a Service Policy](#)" section.



Cisco ASA Adaptive Security Appliances

Industry Certifications and Evaluations

The
Vision
to Succeed



- Common Criteria

- Completed: EAL4, v7.0.6—ASA 5510/20/40 (FW)
- Completed: EAL2, v6.0—ASA SSM-10/20 (IPS)
- In process: EAL4+, v7.2.2—ASA Family (FW)
- In process: EAL4, v7.2.2—ASA Family (VPN)

- FIPS 140

- Completed: Level 2, v7.0.4—ASA Family
- Completed: Level 2, v7.2.2
- In process: Level 2, v8.0.2

- ICSA Firewall 4.1, Corporate Category

- Completed: v7.2.2—ASA Family

- ICSA IPsec 1.0D

- Completed: v7.0.4—ASA Family

- ICSA Anti-Virus Gateway

- Completed: v7.1—ASA Family

- NEBS Level 3

- Completed: ASA 5510, 5520, and 5540



Device List

Add Delete Connect

2.2.2.1
192.168.100.1
70.246.200.117
12.28.59.130
11.11.11.3
24.107.92.53
70.246.200.111

Home

Device Dashboard

Firewall Dashboard

Device Information

General

License

Host Name: **asa-remote**ASA Version: **8.0(3)**Device Uptime: **30d 20h 4m 47s**ASDM Version: **6.0(3)**Device Type: **ASA 5510**Firewall Mode: **Routed**Context Mode: **Single**Total Flash: **64 MB**Total Memory: **256 MB**

Interface Status

Interface	IP Address/Mask	Line	Link
inside	11.11.11.3/24	↑ up	↑ up
outside	70.246.200.111/27	↑ up	↑ up

Select an interface to view input and output Kbps

VPN Tunnels

IKE: 0

IPsec: 0

Clientless SSL VPN: 0

SSL VPN Client: 0

System Resources Status

CPU

CPU Usage (percent)

11%

15:34:27



Memory

Memory Usage (MB)

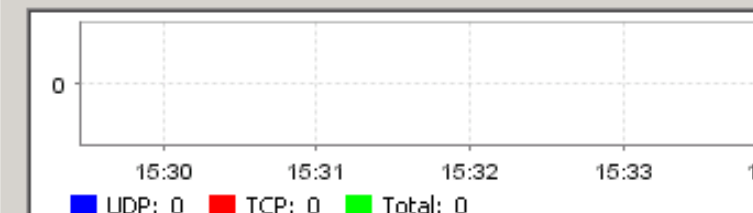
185MB

15:34:27

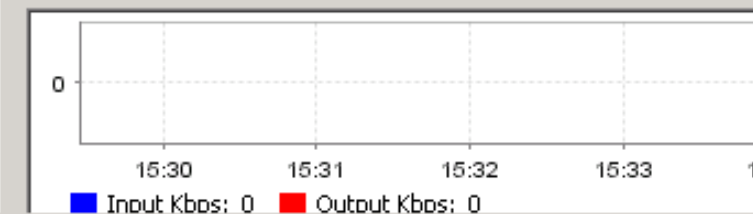


Traffic Status

Connections Per Second Usage

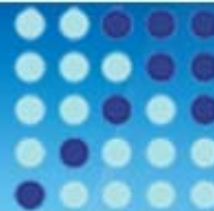


'outside' Interface Traffic Usage (Kbps)



Latest ASDM Syslog Messages

Severity	Date	Time	Syslog ID	Source IP	Destination IP	Message
6	Mar 10 2008	15:34:34	106015	198.200.139.3	70.246.200.111	Deny TCP (no connection) from 198.200.139.3/14300 to 70.246.200.111
6	Mar 10 2008	15:34:34	302014	198.200.139.3	70.246.200.111	Teardown TCP connection 127412 for outside:198.200.139.3/14300 to 70.246.200.111
6	Mar 10 2008	15:34:34	725007	198.200.139.3		SSL session with client outside:198.200.139.3/14300 terminated
6	Mar 10 2008	15:34:34	605005	198.200.139.3	70.246.200.111	Login permitted from 198.200.139.3/14300 to outside:70.246.200.111



Cisco Security Manager Integrated Security Configuration Management



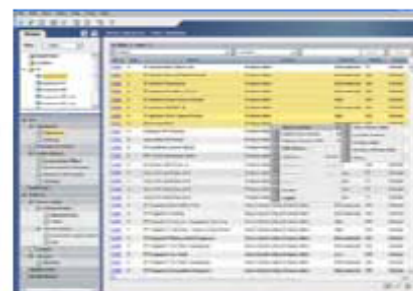
Firewall Management

- Support for Cisco® PIX® Firewall, Cisco Adaptive Security Appliance (ASA), Cisco Firewall Services Module (FWSM), and Cisco IOS® Software Routers
- Rich firewall rule definition: shared objects, rule grouping, and inheritance
- Powerful analysis tools: conflict detection, rule combiner, hit counts, ...



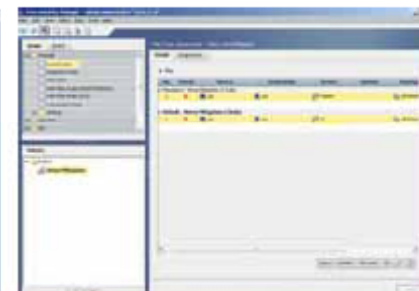
VPN Management

- Support for Cisco PIX Firewall, Cisco ASA, VPN services module (VPNSM), VPN shared port adapter (SPA), and Cisco IOS Software routers
- Support for wide array of VPN technologies, such as DMVPN, Easy VPN, and SSL VPN
- VPN wizard for 3-step point-and-click VPN creation



IPS Management

- Support for IPS sensors and Cisco IOS IPS
- Automatic policy-based IPS sensor software and signature updates
- Signature update wizard allowing easy review and editing prior to deployment



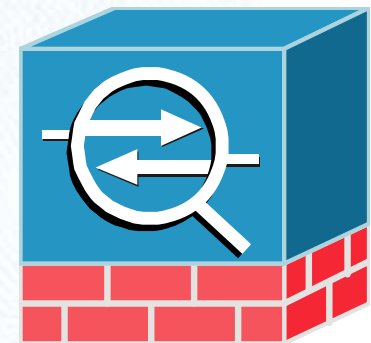
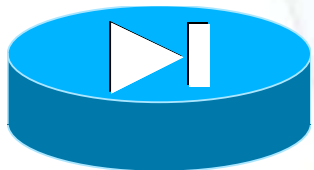
Productivity

- Unified security management for Cisco devices supporting firewall, VPN, and IPS
- Efficient management of up to 5000 devices per server
- Multiple views for task optimization
 - Device view
 - Policy view
 - Topology view





3 Simple Steps



Migrating from the Cisco PIX Firewall to the Cisco ASA Adaptive Security Appliance

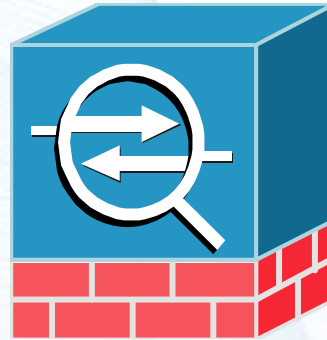


- 1 Upgrade the PIX software version to 7.0.**
- 2 Copy your configuration from the PIX to the ASA.**
- 3 Configure the ASA interfaces.**



Migrating from the Cisco PIX Firewall to the Cisco ASA Security Appliance.

The
Vision
to Succeed



Upgrade to Pix Version 7.0 is seamless and requires little manual intervention. 6.X commands are automatically converted to 7.0 commands.

BUT !!!!!





Also !!!! Before you begin:

1. Backup your configuration 2 times. Once to a text file and once to a TFTP server.
2. Make certain you do not have CONDUIT or OUTBOUND commands. (use output interpreter to convert to access-lists if you do)
3. Make certain the PIX does not terminate PPTP connections. 7.0 does not support PPTP.
4. Save Digital certificates off the PIX if you are using them before beginning the upgrade.
5. After the upgrade make certain to use common sense and confirm the automatic configuration changes have actually occurred.
6. Save the changed configuration to FLASH after the PIX has restarted and converted the configuration.



Which PIX Firewalls CAN and can NOT be upgraded to 7.0



PIX 515



PIX 515E



PIX 525



PIX 535



PIX 501



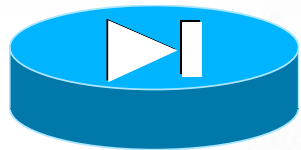
PIX 506



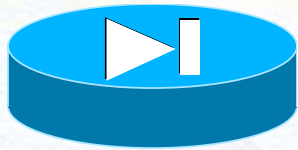
PIX 506E



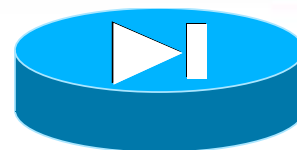
Check the Memory Requirements on the Pix before upgrading.



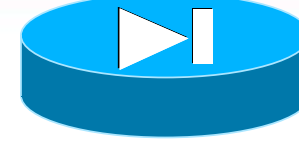
PIX 515



PIX 515E



PIX 525



PIX 535

```
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum: 50ff5d2e11b120e67116711d5e097190
```



```
: end
pix1# show vers
```

Cisco PIX Firewall

Compiled on Thu

pix1 up 38 mins

Amount of RAM:		
model	with restricted license	with unrestricted license
515/515E	64 MB	128 MB
525	128 MB	256 MB
535	512 MB	1 GB

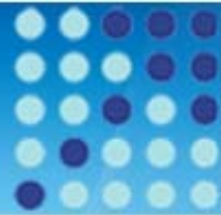
Hardware: PIX-515, 128 MB RAM, CPU Pentium 200 MHz

Flash i28F640J5 @ 0x300, 16MB

BIOS Flash AT29C257 @ 0xffffd8000, 32KB

```
0: ethernet0: address is 0050.54fe.ea68, irq 10
1: ethernet1: address is 0050.54fe.ea69, irq 7
2: ethernet2: address is 00e0.b604.23e1, irq 11
3: ethernet3: address is 00e0.b604.23e0, irq 11
4: ethernet4: address is 00e0.b604.23df, irq 11
5: ethernet5: address is 00e0.b604.23de, irq 11
License_
```





Also !!!! Before you begin:

If you are upgrading a PIX 515 or 535 with PDM already installed

- The PIX Version 6.3 image on a PIX 515 or PIX 535 only accesses the first 8 MB of Flash memory, instead of the entire 16 MB of Flash. If the PIX Security appliance Version 7.0 image in combination with the Flash memory contents exceeds the 8 MB limit, following error message may result: **Insufficient flash space available for this request.** The solution is to load the image from monitor mode. See the “Upgrading in Monitor Mode” section on page 71.
- The PDM image in Flash memory is not automatically copied to the new filesystem. For information about installing ASDM (which replaces PDM on Version 7.0), see the ASDM Release Notes.
- To avoid installation failures, make sure that you have read the “Prerequisites to Upgrading” section on page 63 before proceeding.
- See the “Upgrade Examples” section on page 74 for configuration examples. These will be useful to review before you start your upgrade procedure.



Migrating from the Cisco PIX Firewall to the Cisco ASA security Appliance



Read the following Documents and print them out for reference to make certain you understand the new, changed and deprecated commands.

1. Release notes for the software version for which you plan to upgrade. (7.0)
2. Guide for PIX 6.2 and 6.3 upgrading to Cisco PIX software Version 7.0



Migrating from the Cisco PIX Firewall to the Cisco ASA security Appliance

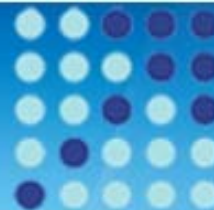
The
Vision
to Succeed



Study the new and deprecated changes !!!



Migrating from the Cisco PIX Firewall to the Cisco ASA security Appliance



PIX Version 6.3	PIX Security appliance Version 7.0
fixup protocol esp-ike	Not Supported
fixup protocol dns maximum-length 512	class-map inspection_default
fixup protocol h323 h225 1720	match default-inspection-traffic
fixup protocol http 80	policy-map global_policy
fixup protocol rsh 514	class inspection_default
fixup protocol sip 5060	inspect ftp
fixup protocol smtp 25	inspect h323 h225
fixup protocol ftp 21	inspect h323 ras
fixup protocol h323 ras 1718-1719	inspect ils
fixup protocol ils 389	inspect rsh
fixup protocol rtsp 554	inspect rtsp
fixup protocol skinny 2000	inspect smtp
fixup protocol sqlnet 1521	inspect sqlnet
	inspect sip
	inspect skinny

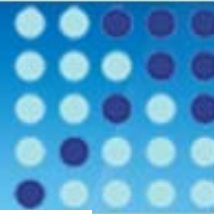
PIX Version 6.3	PIX Security appliance Version 7.0
interface ethernet0 auto	interface Ethernet0
interface ethernet1 auto	nameif outside
interface ethernet1 vlan101 logical	security-level 0
interface ethernet1 vlan102 physical	ip address 171.45.0.13
interface ethernet2 auto shutdown	interface Ethernet1
	no nameif
nameif ethernet0 outside security0	no security-level
nameif vlan101 dmz security50	no ip address
nameif vlan102 inside security100	interface Ethernet1.101
	vlan 101
ip address outside 171.45.0.13	nameif dmz
ip address dmz 10.1.32.12	security-level 50
ip address inside 192.168.15.12	ip address 10.1.32.12
	interface Ethernet1.102
	vlan 102
	nameif inside
	security-level 100
	ip address 192.168.15.12
	interface Ethernet2
	shutdown
	no nameif
	no security-level
	no ip address

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
ca	ca authenticate <ca_nickname> [<i><fingerprint></i>]	crypto ca authenticate <trustpoint> [fingerprint <hex value>] [nointeractive]	—
	[no] ca crl request <ca_nickname>	crypto ca crl request <trustpoint>	—
	[no] ca enroll <ca_nickname> <challenge_password> [serial] [ipaddress]	crypto ca trustpoint <name> [no] ip-address <address> [no] serial-number password <password> exit crypto ca enroll <name>	—
	ca generate rsa (key specialkey) <key_modulus_size>	crypto key generate rsa [usage-keys general-keys] [label <key-pair-label>] [modulus <size>] [noconfirm]	—
	[no] ca identity <ca_nickname> [<ca_ipaddress> <hostname>] [<ca_script_location>] [<ldap_ip address> <hostname>]	crypto ca trustpoint <name> enroll url <ip_address>[hostname]:[<ca_script_location>] crl ldap_defaults <ldap_ip>[hostname] exit	—
	[no] ca save all	Not supported	Certificates and keys will be saved whenever the configuration is saved
	[no] ca subject-name <ca_nickname> <X.500_string>	crypto ca trustpoint <name> [no] subject-name <X.500 string>	—
	ca zeroize rsa [<keypair_name>]	crypto key zeroize rsa[dsa] [label <key-pair-label>] [noconfirm]	—

Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
	ca generate rsa key <modulus>	crypto key generate rsa [usage-keys general-keys] [label <key-pair-label>] [modulus <size>] [noconfirm]	—
	ca generate rsa specialkey <size>	crypto key generate rsa usage-keys modulus <size>	—
	[no] ca configure <ca_nickname> ca ra <retry_period> <retry_count> [crloptional]	crypto ca trustpoint <trustpoint name> enrollment retry period <minutes> enrollment retry count <num> crl configure	The retry period and count are configured via the trustpoint configuration mode. The configuration is an additional configuration mode accessible from the trustpoint configuration mode.
	[no] ca verificertdn <x.500 string>	crypto ca verificertdn <x.500 string>	—



Migrating from the Cisco PIX Firewall to the Cisco ASA security Appliance



Command	PIX Version 6.3	PIX Security appliance Version	Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes
isakmp	isakmp keepalive <seconds> [[<retry-seconds>]	tunnel-group <group name> t; ipsec-ra ipsec-l2l tunnel-group <group name> ipsec-attributes isakmp keepalive [thresh <seconds>][<retry <seconds>]	vpdn	vpdn group <group_name> pptp echo <echo_time>	Not supported	PPTP is not supported in PIX Security appliance Version 7.0
	isakmp key <keystring> address <peer-address> [netmask <mask>] [no-xauth] [no-config-mode]	tunnel-group <group name> t; ipsec-l2l tunnel-group <group name> ipsec-attributes pre-shared-key <preshare>		vpdn group <group_name> accept dialin l2tp	Not supported	L2TP and L2TP over IPSec are not supported in PIX Security appliance Version 7.0.
	isakmp client configuration address-pool local <pool-name> [<interface-name>]	tunnel-group <group name> t; ipsec-l2l tunnel-group <group name> general-attributes address-pool [(interface name)] <address_pool1> ...		vpdn group <group_name> accept dialin pptp	Not supported	PPTP is not supported in PIX Security appliance Version 7.0
				vpdn group <group_name> [client configuration address local <address_pool_name>]	Not supported	—
		vpdn group <group_name> client configuration <dns dns_ip1> [<dns_ip2>]		Not supported	—	
		vpdn group <group_name> client wins_ip1>		Not supported	—	
Command	PIX Version 6.3	PIX Security appliance Version 7.0	Notes	ime> client l aaa	Not supported	—
vpngroup	vpngroup <group_name> address-pool <pool_name>	tunnel-group <group name> type ipsec-l2l tunnel-group <group name> general-attributes address-pool [(interface name)] <address_pool1> [...<address_pool6>]	Converted to tunnel-group syntax	ime> client l_aaa_group>	Not supported	—
	vpngroup <group_name> authentication-server <servers>	Not supported	Used on PIX Version 6.3 to pass a AAA server address for Individual User Authentication (IUA), a feature used on the hardware client; PIX Security appliance Version 7.0 proxies the AAA request for the hardware client, and therefore always sends its own address.	ime>	Not supported	—
				>>	Not supported	Not needed; all PPP traffic is encapsulated by IPSec
				ime> ppp chap mschap	Not supported	—
				ime> ppp 128 auto	Not supported	Not needed; all PPP traffic is encapsulated by IPSec
				sts state rt]	Not supported	Functionality replaced by vpn-sessiondb command



Migrating from the Cisco PIX Firewall to the Cisco ASA security Appliance



1. Plan to perform the Migration during downtime (Although it is an easy 3 step process this is a major change and will require some downtime)
2. Prepare ahead of time by downloading the PIX 7.0 software and putting it on an available TFTP server. Save your existing configuration files and operating system to a TFTP server on the network.

Migrating from the Cisco PIX Firewall to the Cisco ASA Adaptive Security Appliance

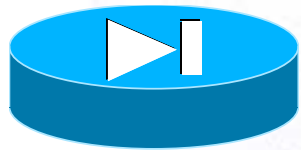


- 1 Upgrade the PIX software version to 7.0.**
- 2 Copy your configuration from the PIX to the ASA.**
- 3 Configure the ASA interfaces.**

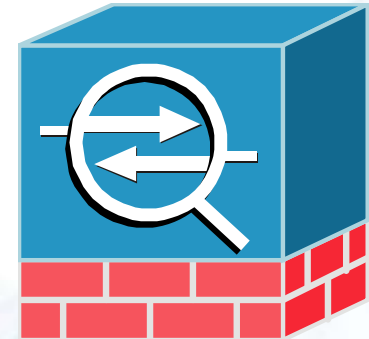


Migrating from the Cisco PIX Firewall to the Cisco ASA security Appliance

The
Vision
to Succeed



Step 1




Upgrade your Pix Firewall Software Version from version 6.2 or 6.3 to Pix Software Version 7.0.





Step 1a:

Verify you are running Pix 6.2 or 6.3 and you have enough RAM for the upgrade to 7.X



```
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:59ff5d2c44b420c671467d4d5ac87480
: end
pix1# show version

Cisco PIX Firewall Version 6.3(5)

Compiled on Thu 04-Aug-05 21:40 by morlee

pix1 up 38 mins 49 secs

Hardware:   PIX-515, 128 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xffffd8000, 32KB

0: ethernet0: address is 0050.54fe.ea68, irq 10
1: ethernet1: address is 0050.54fe.ea69, irq 7
2: ethernet2: address is 00e0.b604.23e1, irq 11
3: ethernet3: address is 00e0.b604.23e0, irq 11
4: ethernet4: address is 00e0.b604.23df, irq 11
5: ethernet5: address is 00e0.b604.23de, irq 11
License_
```

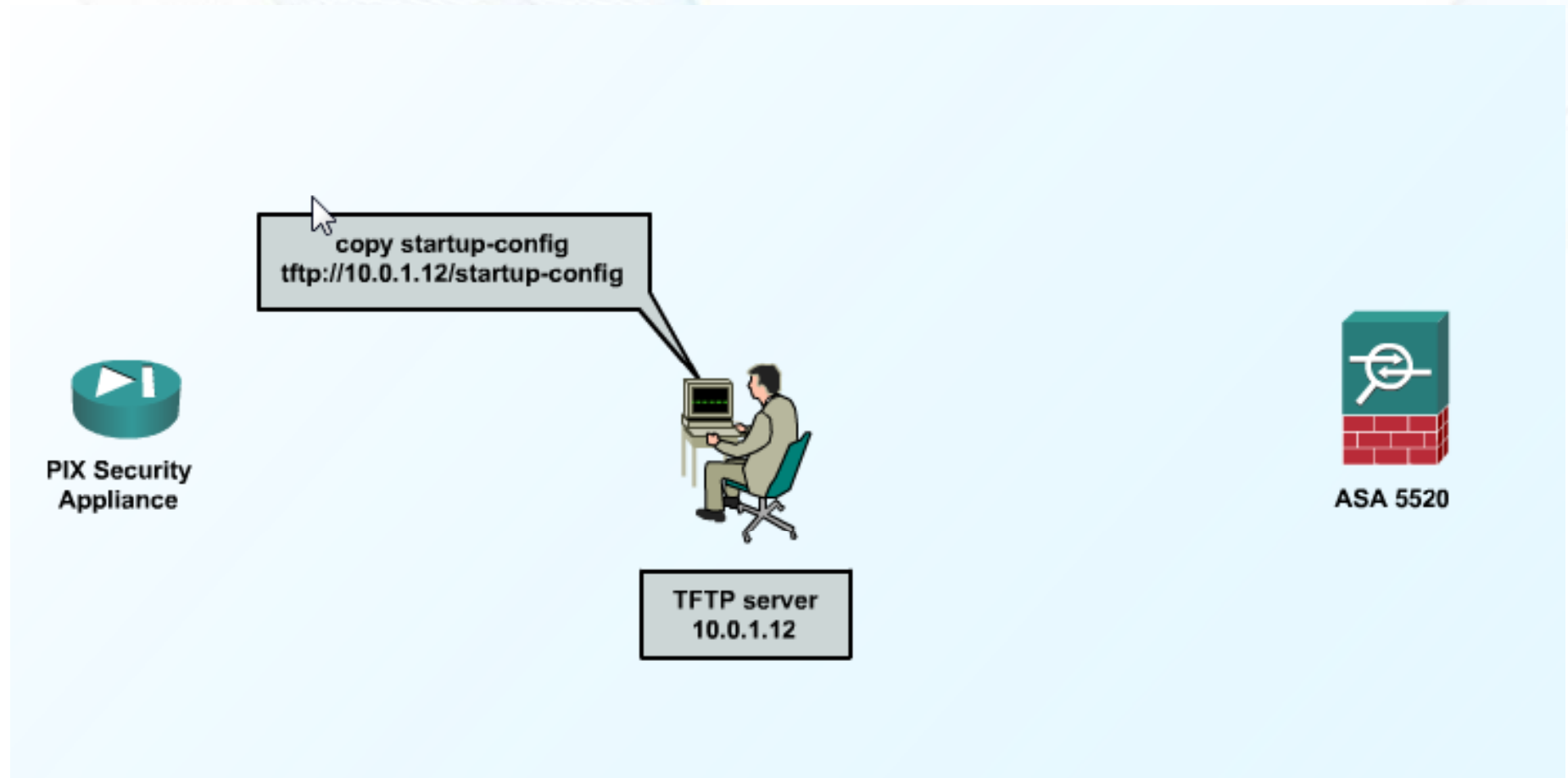
Software version: 6.2 or 6.3



Step 1b:



Save your current configuration and current operating system to a TFTP server on the network.



Have a Recovery Plan before you begin



Step 1b: (cont'd)



```
Inside Hosts      : Unlimited
Failover          : Active/Active
VPN-DES           : Enabled
VPN-3DES-AES      : Enabled
Cut-through Proxy : Enabled
Guards            : Enabled
URL Filtering     : Enabled
Security Contexts : 2
GTP/GPRS          : Disabled
VPN Peers         : Unlimited
```

This platform has an Unrestricted (UR) license.

Serial Number: 403340064

Running Activation Key: 0x66c7ca88 0x6b0681f6 0x017defa8 0xb06f0dec

Configuration has not been modified since last system restart.

pix1# copy startup-config tftp://10.0.1.12/startup-config

Address or name of remote host [10.0.1.12]?

Destination filename [startup-config]?

!

2147 bytes copied in 0.180 secs

pix1#



Step 1b



Rename the **"OLD"** backup configuration file appropriately so that it is not confused with the **"NEW"** converted 7.0 configuration that you will also be copying to the TFTP server.

Example: startup-config.old



Step 1c:



Copy the. new 7.0 code to your PIX from the TFTP server

```
1: ethernet1: address is 0050.54fe.ea69, irq 7
2: ethernet2: address is 00e0.b604.23e1, irq 11
3: ethernet3: address is 00e0.b604.23e0, irq 11
4: ethernet4: address is 00e0.b604.23df, irq 11
5: ethernet5: address is 00e0.b604.23de, irq 11
```

License Features:

Failover:	Enabled
VPN-DES:	Enabled
VPN-3DES-AES:	Enabled
Maximum Physical Interfaces:	6
Maximum Interfaces:	10
Cut-through Proxy:	Enabled
Guards:	Enabled
URL-filtering:	Enabled
Inside Hosts:	Unlimited
Throughput:	Unlimited
IKE peers:	Unlimited

This PIX has an Unrestricted (UR) license.

Serial Number: 403340064 (0x180a7b20)

Running Activation Key: 0x66c7ca88 0x6b0681f6 0x017defa8 0xb06f0dec

Configuration has not been modified since last system restart.

pix1# copy tftp flash:image





Step 1c: (cont'd)

```
2: ethernet2: address is 00e0.b604.23e1, irq 11
3: ethernet3: address is 00e0.b604.23e0, irq 11
4: ethernet4: address is 00e0.b604.23df, irq 11
5: ethernet5: address is 00e0.b604.23de, irq 11
```

Licensed Features:

```
Failover: Enabled
VPN-DES: Enabled
VPN-3DES-AES: Enabled
Maximum Physical Interfaces: 6
Maximum Interfaces: 10
Cut-through Proxy: Enabled
Guards: Enabled
URL-filtering: Enabled
Inside Hosts: Unlimited
Throughput: Unlimited
IKE peers: Unlimited
```

This PIX has an Unrestricted (UR) license.

Serial Number: 403340064 (0x180a7b20)

Running Activation Key: 0x66c7ca88 0x6b0681f6 0x017defa8 0xb06f0dec

Configuration has not been modified since last system restart.

pix1# copy tftp flash:image

Address or name of remote host [0.0.0.0]? 10.0.1.12





Step 1c: (cont'd)

```
3: ethernet3: address is 00e0.b604.23e0, irq 11
4: ethernet4: address is 00e0.b604.23df, irq 11
5: ethernet5: address is 00e0.b604.23de, irq 11
```

Licensed Features:

```
Failover: Enabled
VPN-DES: Enabled
VPN-3DES-AES: Enabled
Maximum Physical Interfaces: 6
Maximum Interfaces: 10
Cut-through Proxy: Enabled
Guards: Enabled
URL-filtering: Enabled
Inside Hosts: Unlimited
Throughput: Unlimited
IKE peers: Unlimited
```

This PIX has an Unrestricted (UR) license.

Serial Number: 403340064 (0x180a7b20)

Running Activation Key: 0x66c7ca88 0x6b0681f6 0x017defa8 0xb06f0dec

Configuration has not been modified since last system restart.

pix1# copy tftp flash:image

Address or name of remote host [0.0.0.0]? 10.0.1.12

Source file name [cdisk]? **pix702.bin**





Step 1c: (cont'd)

5: ethernet5: address is 00e0.b604.23de, irq 11

Licensed Features:

Failover:	Enabled
VPN-DES:	Enabled
VPN-3DES-AES:	Enabled
Maximum Physical Interfaces:	6
Maximum Interfaces:	10
Cut-through Proxy:	Enabled
Guards:	Enabled
URL-filtering:	Enabled
Inside Hosts:	Unlimited
Throughput:	Unlimited
IKE peers:	Unlimited

This PIX has an Unrestricted (UR) license.

Serial Number: 403340064 (0x180a7b20)

Running Activation Key: 0x66c7ca88 0x6b0681f6 0x017defa8 0xb06f0dec

Configuration has not been modified since last system restart.

pix1# copy tftp flash:image

Address or name of remote host [0.0.0.0]? 10.0.1.12

Source file name [cdisk]? pix702.bin

copying tftp://10.0.1.12/pix702.bin to flash:image

[yes|no|again]? yes



The **08 Vision**
to Succeed

A large grid of 1000 small human figures arranged in 10 rows and 100 columns, illustrating the concept of a large population.

Erasing current image

QUESTION



Step 1d:



Reboot the Pix Firewall (reload)

After the reboot of the Pix Firewall 7.0 code will load and the 6.X configuration will be converted to 7.X commands.

After you upgrade the Pix from 6.X to 7.X use the show startup-config errors command to display the errors experienced converting the 6.X code to 7.X

Save the configuration (wr mem)





What if something goes TERRIBLY wrong !!!



Monitor Mode Upgrade



Hit the “ESCAPE” key right after the Pix begins to boot



```
00 00 00 8086 7192 Host Bridge
00 07 00 8086 7110 ISA Bridge
00 07 01 8086 7111 IDE Controller
00 07 02 8086 7112 Serial Bus          9
00 07 03 8086 7113 PCI Bridge
00 00 00 8086 1209 Ethernet          11
00 0E 00 8086 1209 Ethernet          10
00 11 00 8086 1229 Ethernet          11
```

```
Cisco Secure PIX Firewall BIOS (4.2) #0: Mon Dec 31 08:34:35 PST 2001
Platform PIX-515E
System Flash=E28F128J3 @ 0xffff00000
```

```
Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Flash boot interrupted.
```

```
0: i8255X @ PCI(bus:0 dev:14 irq:10)
1: i8255X @ PCI(bus:0 dev:13 irq:11)
2: i8255X @ PCI(bus:0 dev:17 irq:11)
```

```
Ethernet auto negotiation timed out.
Ethernet port 1 could not be initialized.
Use ? for help.
monitor>
```



Monitor Mode Upgrade



```
monitor>  
monitor>  
monitor>  
monitor>  
monitor>  
monitor>  
monitor>  
monitor>  
monitor>  
monitor>  
monitor>  
monitor>  
monitor>  
monitor>  
monitor>  
monitor> interface 1  
0: i8255X @ PCI(bus:0 dev:14 irq:10)  
1: i8255X @ PCI(bus:0 dev:13 irq:11)  
2: i8255X @ PCI(bus:0 dev:17 irq:11)  
  
Ethernet auto negotiation timed out.  
Ethernet port 1 could not be initialized.  
monitor>  
monitor>
```



Monitor Mode Upgrade



```
monitor> address 1.1.1.1  
address 1.1.1.1  
monitor>  
monitor> address 1.1.1.1 255.255.255.0  
address 1.1.1.1  
monitor>
```



Monitor Mode Upgrade



```
monitor>  
monitor>  
monitor>  
monitor>  
monitor>  
monitor>  
monitor> interface 1  
0: i8255X @ PCI(bus:0 dev:14 irq:10)  
1: i8255X @ PCI(bus:0 dev:13 irq:11)  
2: i8255X @ PCI(bus:0 dev:17 irq:11)
```

```
Ethernet auto negotiation timed out.  
Ethernet port 1 could not be initialized.
```

```
monitor>  
monitor> gateway 1.1.1.254  
gateway 1.1.1.254  
monitor>
```



Monitor Mode Upgrade



```
monitor /  
monitor>  
monitor> interface 1  
0: i8255X @ PCI(bus:0 dev:14 irq:10)  
1: i8255X @ PCI(bus:0 dev:13 irq:11)  
2: i8255X @ PCI(bus:0 dev:17 irq:11)  
  
Ethernet auto negotiation timed out.  
Ethernet port 1 could not be initialized.  
monitor>  
monitor> gateway 1.1.1.254  
gateway 1.1.1.254  
monitor> file pix707.bin  
file pix707.bin  
monitor>
```



Monitor Mode Upgrade



```
monitor /
monitor>
monitor> interface 1
0: i8255X @ PCI(bus:0 dev:14 irq:10)
1: i8255X @ PCI(bus:0 dev:13 irq:11)
2: i8255X @ PCI(bus:0 dev:17 irq:11)

Ethernet auto negotiation timed out.
Ethernet port 1 could not be initialized.
monitor>
monitor> gateway 1.1.1.254
gateway 1.1.1.254
monitor> file pix707.bin
file pix707.bin
monitor> server 1.1.1.22
server 1.1.1.22
monitor>
```



Monitor Mode Upgrade



```
monitor> address 1.1.1.1  
address 1.1.1.1  
monitor>  
monitor> address 1.1.1.1 255.255.255.0  
address 1.1.1.1  
monitor> tftp  
tftp pix707.bin@1.1.1.22 via 1.1.1.254_
```



!!! Congratulations !!!

You have finished STEP #1.



You have upgraded the code on your existing Pix Firewall to 7.0. By doing this you have automatically converted your configuration from 6.X commands to the new 7.X commands.





Step 2



Copy your converted configuration on the Cisco PIX Firewall to the Cisco ASA Adaptive Security Appliance.

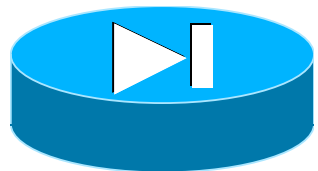


Step 2:

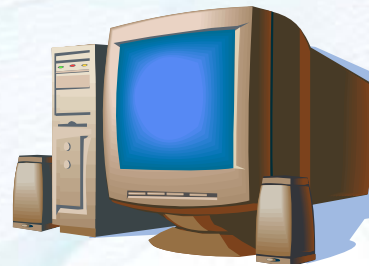


Copy the configuration from the PIX to the ASA.

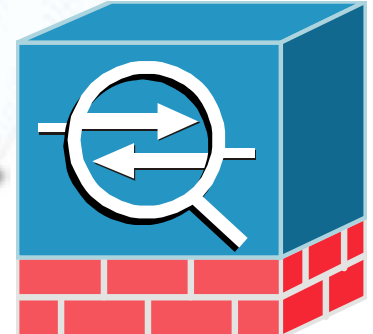
Copy the configuration from the PIX to a TFTP server. Then use the copy command to download the configuration from the TFTP server to the ASA.



PIX



TFTP Server



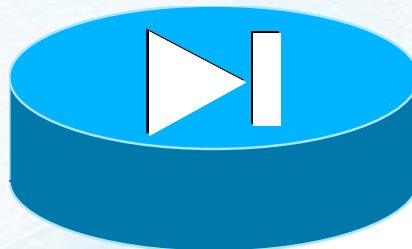
ASA



Step 2:



Go to the PIX Firewall



Step 2a:



Move the 7.X configuration from the PIX to the TFTP server

```
3: Ext: Ethernet3      : address is 00e0.b604.23e0, irq 11
4: Ext: Ethernet4      : address is 00e0.b604.23df, irq 11
5: Ext: Ethernet5      : address is 00e0.b604.23de, irq 11
```

Licensed features for this platform:

```
Maximum Physical Interfaces : 6
Maximum VLANs               : 25
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL Filtering                : Enabled
Security Contexts           : 2
GTP/GPRS                    : Disabled
VPN Peers                   : Unlimited
```

This platform has an Unrestricted (UR) license.

Serial Number: 403340064

Running Activation Key: 0x66c7ca88 0x6b0681f6 0x017defa8 0xb06f0dec

Configuration has not been modified since last system restart.

pix1# copy startup-config tftp://10.0.1.12/startup-config



Step 2a:



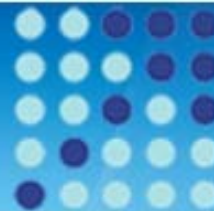
Good thing we renamed our **old** configuration file

From startup-config

To: startup-config.old



Step 2a: (Cont'd)



Copy the 7.X configuration from the PIX to the TFTP server

```
5: Ext: Ethernet5          : address is 00e0.b604.23de, irq 11
```

```
Licensed features for this platform:
```

```
Maximum Physical Interfaces : 6  
Maximum VLANs               : 25  
Inside Hosts                 : Unlimited  
Failover                    : Active/Active  
VPN-DES                      : Enabled  
VPN-3DES-AES                 : Enabled  
Cut-through Proxy           : Enabled  
Guards                      : Enabled  
URL Filtering                : Enabled  
Security Contexts           : 2  
GTP/GPRS                    : Disabled  
VPN Peers                   : Unlimited
```

```
This platform has an Unrestricted (UR) license.
```

```
Serial Number: 403340064
```

```
Running Activation Key: 0x66c7ca88 0x6b0681f6 0x017defa8 0xb06f0dec
```

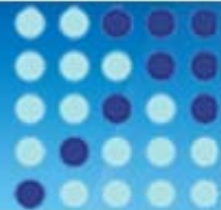
```
Configuration has not been modified since last system restart.
```

```
pix1# copy startup-config tftp://10.0.1.12/startup-config
```

```
Address or name of remote host [10.0.1.12]? 10.0.1.12
```



Step 2a: (Cont'd)



Copy the 7.X configuration from the PIX to the TFTP server

Licensed features for this platform:

```
Maximum Physical Interfaces : 6
Maximum VLANs               : 25
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Enabled
Cut-through Proxy            : Enabled
Guards                       : Enabled
URL Filtering                 : Enabled
Security Contexts            : 2
GTP/GPRS                     : Disabled
VPN Peers                    : Unlimited
```

This platform has an Unrestricted (UR) license.

Serial Number: 403340064

Running Activation Key: 0x66c7ca88 0x6b0681f6 0x017defa8 0xb06f0dec

Configuration has not been modified since last system restart.

```
pix1# copy startup-config tftp://10.0.1.12/startup-config
```

Address or name of remote host [10.0.1.12]?

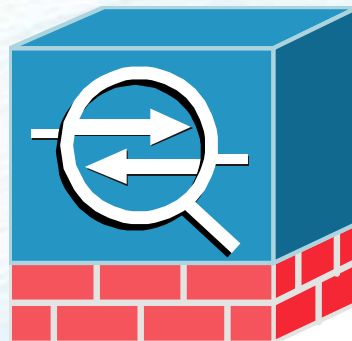
Destination filename [startup-config]? _



Step 2:



Go to the new ASA



Step 2b:



Copy the 7.X configuration from the TFTP Server to the ASA Security Appliance

```
!  
policy-map global_policy  
  class inspection_default  
    inspect dns maximum-length 512  
    inspect ftp  
    inspect h323 h225  
    inspect h323 ras  
    inspect rsh  
    inspect rtsp  
    inspect esmtp  
    inspect sqlnet  
    inspect skinny  
    inspect sunrpc  
    inspect xdmcp  
    inspect sip  
    inspect netbios  
    inspect tftp  
    inspect http  
!  
service-policy global_policy global  
Cryptochecksum:7f551f4b9bb9f39fc405912de50bcf6e  
: end  
asa1# copy tftp://10.0.1.12/startup-config startup-config
```



Step 2b: (Cont'd)

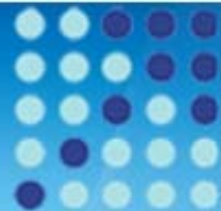


Copy the 7.X configuration from the TFTP Server to the ASA Security Appliance.

```
policy-map global_policy
  class inspection_default
    inspect dns maximum-length 512
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect esmtp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect sip
    inspect netbios
    inspect tftp
    inspect http
  !
service-policy global_policy global
Cryptochecksum:7f551f4b9bb9f39fc405912de50bcf6e
: end
asa1# copy tftp://10.0.1.12/startup-config startup-config
Address or name of remote host [10.0.1.12]?
```



Step 2b: (Cont'd)



Copy the 7.X configuration from the TFTP Server to the ASA Security Appliance.

```
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect http
!
service-policy global_policy global
Cryptochecksum:7f551f4b9bb9f39fc405912de50bcf6e
: end
asa1# copy tftp://10.0.1.12/startup-config startup-config

Address or name of remote host [10.0.1.12]?

Source filename [startup-config]?
```



Step 2b: (Cont'd)



Copy the 7.X configuration from the TFTP Server to the ASA Security Appliance.

```
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect http
!
service-policy global_policy global
Cryptochecksum:7f551f4b9bb9f39fc405912de50bcf6e
: end
asa1# copy tftp://10.0.1.12/startup-config startup-config

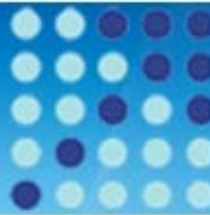
Address or name of remote host [10.0.1.12]?

Source filename [startup-config]?

Accessing tftp://10.0.1.12/startup-config...!
Writing system file...
!
2115 bytes copied in 0.200 secs
asa1# config t
```



Step 2b: (Cont'd)



Copy the 7.X configuration from the TFTP Server to the ASA Security Appliance.

```
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect http
!
service-policy global_policy global
Cryptochecksum:7f551f4b9bb9f39fc405912de50bcf6e
: end
asa1# copy tftp://10.0.1.12/startup-config startup-config

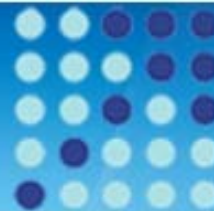
Address or name of remote host [10.0.1.12]?

Source filename [startup-config]?

Accessing tftp://10.0.1.12/startup-config...!
Writing system file...
!
2115 bytes copied in 0.200 secs
asa1# config t
asa1(config)# clear config all
```



Step 2b: (Cont'd)

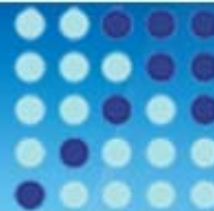


Copy the 7.X configuration from the TFTP Server to the ASA Security Appliance.

```
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect http
!
service-policy global_policy global
Cryptochecksum:7f551f4b9bb9f39fc405912de50bcf6e
: end
asa1# copy tftp://10.0.1.12/startup-config startup-config
Address or name of remote host [10.0.1.12]?
Source filename [startup-config]?
Accessing tftp://10.0.1.12/startup-config...!
Writing system file...
!
2115 bytes copied in 0.200 secs
asa1# config t
asa1(config)# clear config all
ciscoasa(config)# copy start run
```



Step 2b: (Cont'd)



Copy the 7.X configuration from the TFTP Server to the ASA Security Appliance.

```
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect http
!
service-policy global_policy global
Cryptochecksum:7f551f4b9bb9f39fc405912de50bcf6e
: end
asa1# copy tftp://10.0.1.12/startup-config startup-config

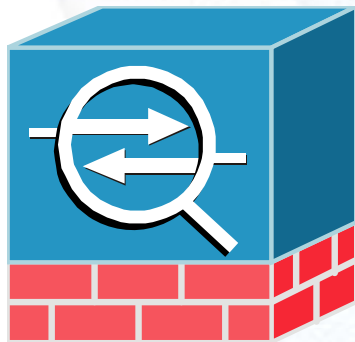
Address or name of remote host [10.0.1.12]?

Source filename [startup-config]?

Accessing tftp://10.0.1.12/startup-config...!
Writing system file...
!
2115 bytes copied in 0.200 secs
asa1# config t
asa1(config)# clear config all
ciscoasa(config)# copy start run

Destination filename [running-config]?
```





Step 3



Configure the ASA interfaces
Names, Security Levels, IP addresses



Step 3:



**Configure the ASA interfaces for IP, name ,
and security level (Notice the errors during conversion)**

```
ERROR: % Invalid input detected at '^' marker.  
monitor-interface HR  
ERROR: % Invalid input detected at '^' marker.  
monitor-interface intf3  
ERROR: % Invalid input detected at '^' marker.  
monitor-interface intf4  
ERROR: % Invalid input detected at '^' marker.  
monitor-interface intf5  
ERROR: % Invalid input detected at '^' marker.  
.WARNING: Policy map global_policy is already configured as a service poli  
Cryptochecksum(changed): 8811ac7a af8f91de 623ca65c bae14a1b  
2115 bytes copied in 6.90 secs (352 bytes/sec)  
pix1(config)# show run
```

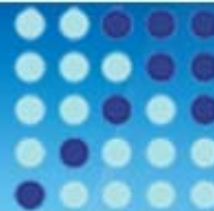




```
interface Ethernet0/0
  nameif outside
  security-level 0
  ip address 70.222.200.111 255.255.255.224
  no shutdown
!
interface Ethernet0/1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
interface Ethernet0/2
  nameif dmz
  security-level 50
  ip address 172.16.1.1 255.255.255.0
  no shutdown
```



Step 3: (Cont'd)



Configure the ASA interfaces for IP, name and security level

```
C:\ Telnet 11.11.11.1
asa-remote#
asa-remote#
asa-remote#
asa-remote#
asa-remote#
asa-remote#
asa-remote#
asa-remote#
asa-remote#
asa-remote#
asa-remote#
asa-remote#
asa-remote#
asa-remote#
asa-remote#
asa-remote# sh int ip br
asa-remote# sh int ip brief
```

Interface	IP-Address	OK?	Method	Status	Prot
Ethernet0/0	70.246.200.111	YES	CONFIG	up	up
Ethernet0/1	11.11.11.3	YES	CONFIG	up	up
Ethernet0/2	unassigned	YES	unset	administratively down	down
Ethernet0/3	unassigned	YES	unset	administratively down	down
Management0/0	unassigned	YES	unset	administratively down	down

```
asa-remote#
```



Step 3: ASA 5505



**Configure the ASA interfaces for IP, name ,
and security level**

```
C:\ Telnet 11.11.11.1

:
ASA Version 8.0(3)
:
hostname asa-in-out
domain-name ccie8521.com
enable password 2KFQnbNIdI.2KY0U encrypted
names
:
interface Vlan1
 nameif inside
 security-level 100
 ip address 2.2.2.1 255.255.255.0
:
interface Vlan2
 nameif outside
 security-level 0
 ip address 70.246.200.117 255.255.255.224
:
interface Ethernet0/0
 switchport access vlan 2
:
interface Ethernet0/1
:
interface Ethernet0/2
<--- More --->
```



Step 3: ASA 5505

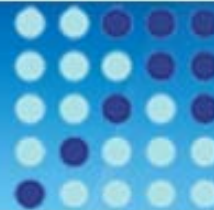


Configure the ASA interfaces for IP, name ,
and security level

```
C:\ Telnet 11.11.11.1
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)# sh switch vlan
VLAN Name
-----
1    inside          up          Et0/1, Et0/2, Et0/3, Et0/4
                Et0/5, Et0/6, Et0/7
2    outside         up          Et0/0
asa-in-out(config)#
```



Step 3: (Cont'd)



Configure the ASA interfaces for IP, name ,
and security level

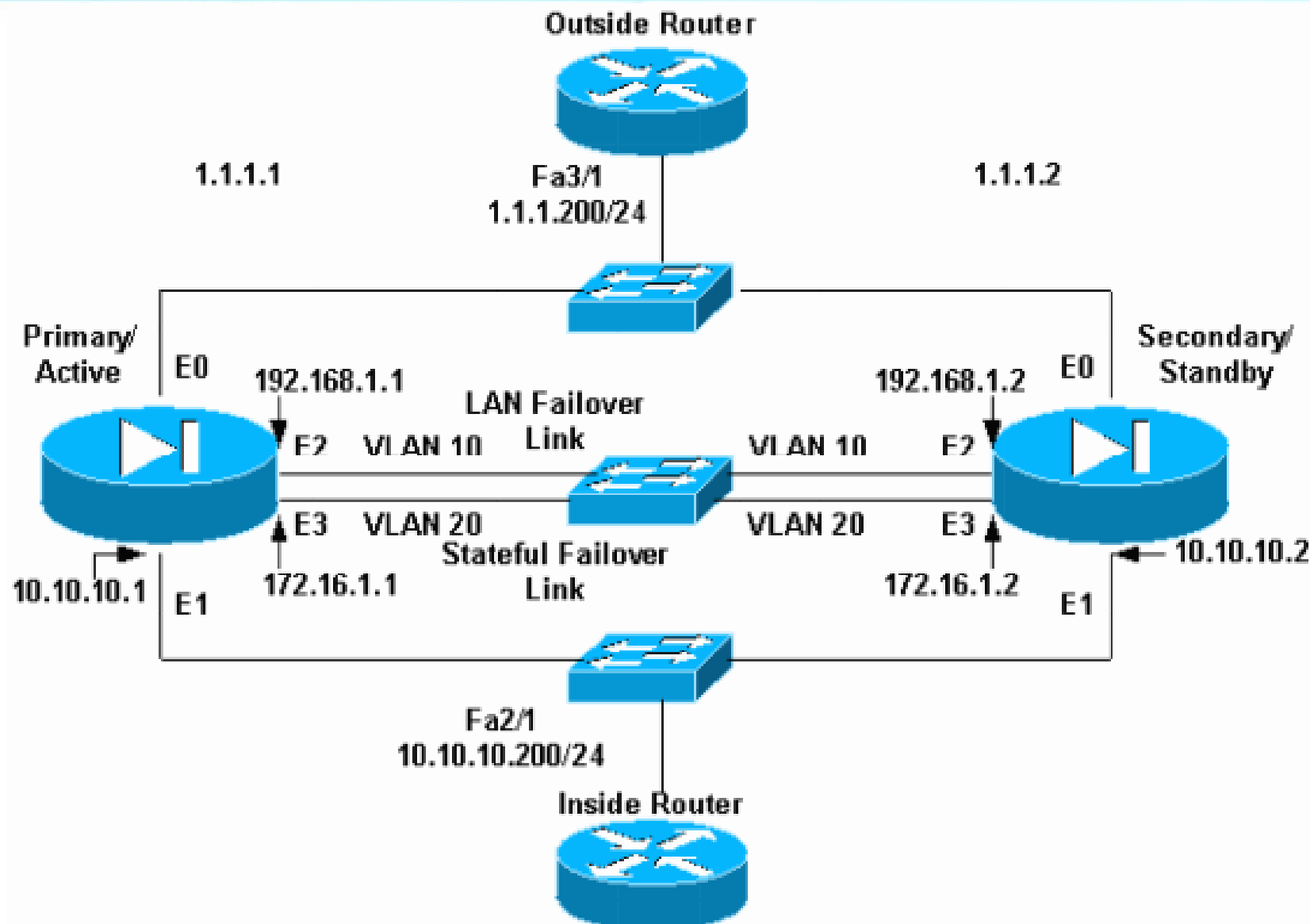
```
Telnet 11.11.11.1
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)#
asa-in-out(config)# sh int ip brief
```

Interface	IP-Address	OK?	Method	Status	Prot
ocol					
Internal-Data0/0	unassigned	YES	unset	up	up
Internal-Data0/1	unassigned	YES	unset	administratively down	up
Loopback0	127.1.0.1	YES	unset	up	up
Vlan1	2.2.2.1	YES	manual	up	up
Vlan2	70.246.200.117	YES	manual	up	up
Ethernet0/0	unassigned	YES	unset	up	up
Ethernet0/1	unassigned	YES	unset	up	up
Ethernet0/2	unassigned	YES	unset	down	down
Ethernet0/3	unassigned	YES	unset	down	down
Ethernet0/4	unassigned	YES	unset	down	down
Ethernet0/5	unassigned	YES	unset	down	down
Ethernet0/6	unassigned	YES	unset	down	down
Ethernet0/7	unassigned	YES	unset	down	down

```
asa-in-out(config)#
```



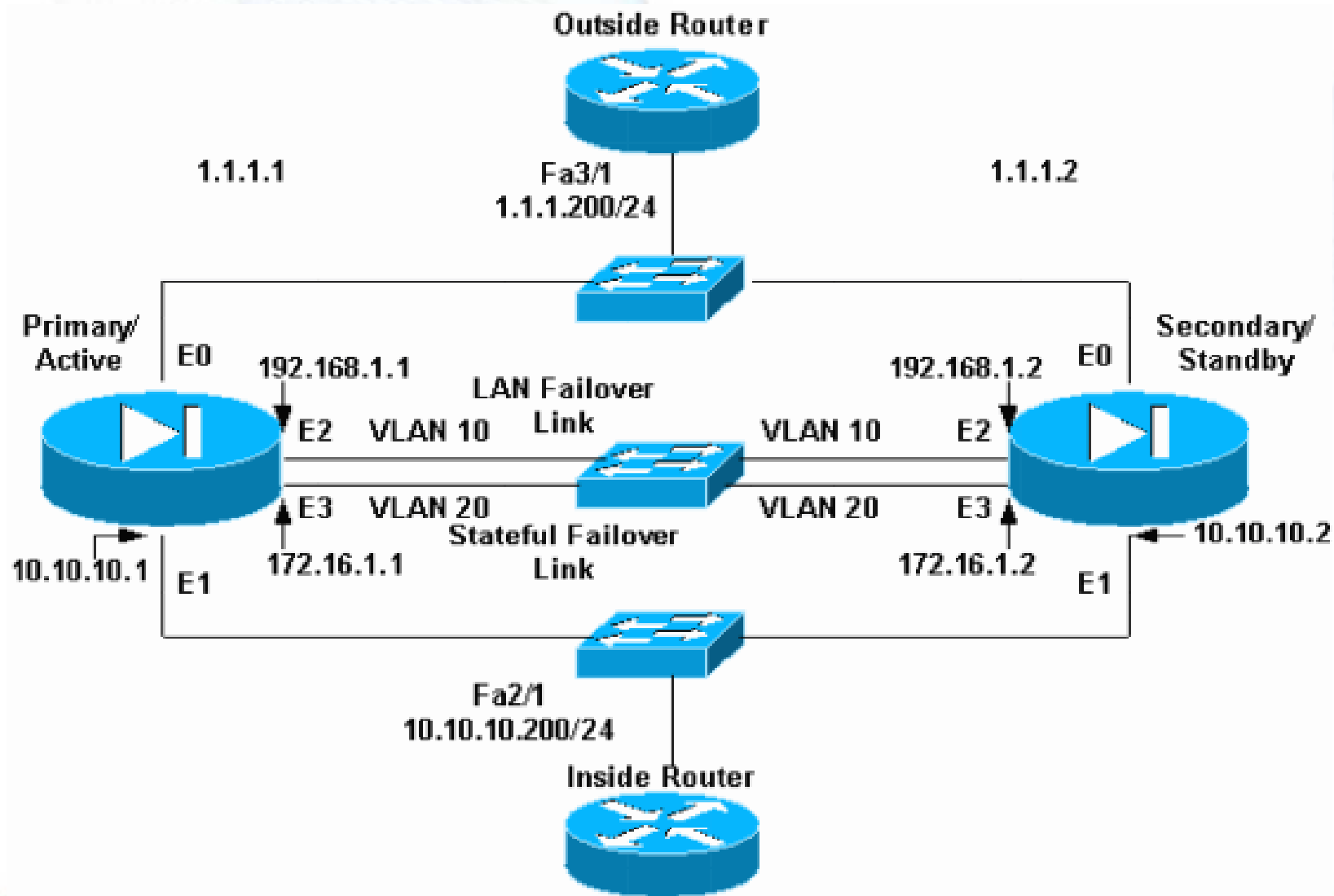
How do I upgrade Upgrading Pix Failover Sets to 7.0 ???



Step 1:



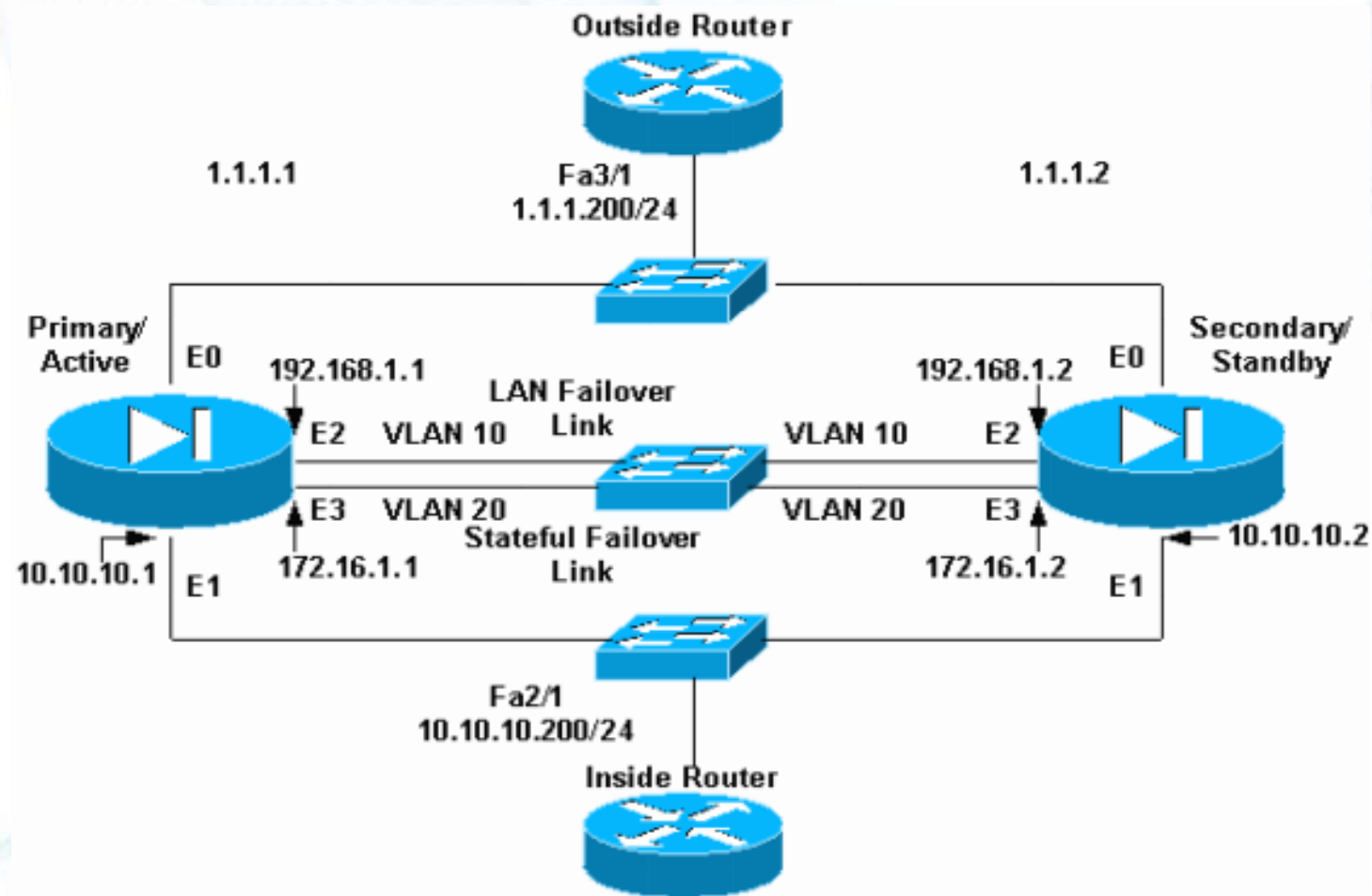
Power Down the Standby\Backup Pix



Step 2:



Upgrade the Active\Powered On Pix to 7.0 as Previously shown in this Demo. Reboot at least once and make certain to verify functionality.



How do I upgrade Upgrading Pix Failover Sets to 7.0 ???



Step 3: Power off the newly upgraded Pix and power on the second Pix and upgrade the second Pix. Verify the upgrade of the second Pix and reboot at least once.

Step 4: Now also power on the First Pix that you upgraded.

Both Pix appliances are now upgraded to 7.0 and are powered on.

Step 5: Use the show failover command to verify that they establish failover communications.



Are there any known issues with upgrading failover sets ????



If you share the Stateful Failover update link with a link for regular traffic such as your inside interface, you must change your configuration before upgrading. Please do not upgrade until you have corrected your configuration, as this is not a supported configuration and PIX Security appliance Version 7.0 treats the LAN failover and Stateful Failover update interfaces as special interfaces.

If you upgrade to PIX Security appliance Version 7.0 with a configuration that shares an interface for both regular traffic and the Stateful Failover updates, configuration related to the regular traffic interface will be lost after the upgrade. The lost configuration may prevent you from connecting to the security appliance over the network.



Summary: Why Migrate to ASA?

The Converged Advantage



- **Superior solution with converged best-of-breed security services**
 - Combines market-proven firewall, IPS, IPSec, and SSL VPN services along with adaptive architecture for future services extensions—protects businesses with its superior network security posture, while providing strong investment protection
- **Threat-protected VPN services**
 - Gives businesses VPN deployment flexibility by offering both IPSec and WebVPN services, allowing businesses to tailor fit secure connectivity services based on their growing connectivity and scalability requirements
- **Consistent user experience**
 - Leverages customers existing knowledge of Cisco PIX Security Appliances for easy migration to Cisco ASA 5500 solutions
- **High-performance IPS and Anti-X Services**
 - Advanced Intrusion Prevention Services (IPS) and network Anti-X Services mitigate wide range of threats including worms, web-based attacks, and more





Expert guidance and support can help improve the accuracy and completeness of migration.

WWT Service Capabilities and Features

- Configuration review and improvement recommendations
- Remote or Onsite knowledge transfer sessions to help you support your migration process
- Focused escalation support during critical migration change windows
- Review of plans for migration, testing, rollback, failure recovery, and risk mitigation, and recommend improvements
- Support for conversion of Cisco PIX Firewall configurations and IPSec VPN configurations to Cisco ASA configurations, providing configuration best practices
- Provide guidance through firewall cutovers





WWT is the only Cisco Gold Partner that is also a Cisco Learning Partner

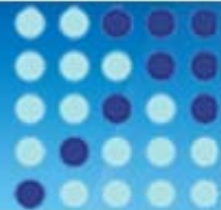
Securing Networks with Pix and ASA (SNPA)

- Taught by Cisco Certified Systems Instructors with real-world deployment experience
- 5-day class with hands-on labs
- Live equipment in Classroom

New ASA Course Offerings:

- New Curriculum focusing on ASA 8.0 to be released in May/June 2008





- Cisco Security Center
<http://tools.cisco.com/security/center/home.x>
- Cisco ASA 5500 Series Adaptive Security Appliances
<http://www.cisco.com/go/asa>
- Cisco PIX Security Appliances End Of Sale Customer Portal
<http://www.cisco.com/go/pixeos>
- Cisco ASA 5500: Power of the PIX Plus
http://www.cisco.com/cdc_content_elements/flash/security/pix500/cisco_asa_flash.html
- Cisco Security Manager
<http://www.cisco.com/en/US/products/ps6498/index.html>
- Additional Resources:
 - For more information about the Cisco End-of-Life Policy, go to:
http://www.cisco.com/en/US/products/prod_end_of_life.html
 - To subscribe to receive end-of-life/end-of-sale information, go to:
<http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice>



Call to Action!!



- Are you ready to Migrate ?
 - Cisco is offering aggressive trade in programs that will allow you to transition at your own pace. Please contact your WWT/Cisco sales account manager for further details.
- WWT Professional Services Offering:
 - Our Experienced Professional Services Engineers are here to provide Expert guidance and support that can help you improve the accuracy and completeness of migration.





Q & A





Thank You !!

